VOLUME 6 ISSN 2456-9704

RIGHT TO PRIVACY AND DATA PROTECTION: INDIAN PERSPECTIVE

By *Sumaiyah Fathima*
From *The Central Law College, Salem, Tamil Nadu*

The manipulation of digitalized storages and transactions in this technological and cashless economy has been rapidly increasing which has instigated India to scrutiny the protection of data and privacy rules by enacting disparate pieces of legislation. Though these laws are not defined exclusively for the data protection, however the courts on several occasions have interpreted 'data protection' with the ambits of 'right to privacy'. As we celebrate the Supreme Court's unanimous verdict on privacy being a fundamental right, it is worth exploring the changing technological landscape within which this right will play out. Now India is waging towards the future call of Robust Regime. While a constitutional right to privacy will undoubtedly limit the states intrusive power over individuals, the full potential of this right will only be realized by data protection laws that will tyrannize how private companies collect and use data.

This paper would focus on the lack of genuinely independent data protection system of regulators and the needs for implementation of legal structure like those followed in other countries and other exhortations that would actually result in the increase of surveillance of individuals, so the trust of public can be maintained.

Keyword: data protection, technology, implementations

Privacy is not an option, and it shouldn't be the price we accept for just getting on internet.
-Gary Kovaus

Introduction

Privacy is a valuable aspect of personality. In modern society, right to privacy has been recognized both in eyes of law and in common parlance. The right to privacy refers to specific right of an individual to control the collection, use and disclosure of personal information. Personal information could be in the form of personal interests, family records, communication records, medical records, and financial records to name a few. The global use of interest for electronic communication and e-commerce over the past few years has become a common phenomenon of modern life. No doubt that it has fascinated our life, but the convergence of innovative technology paves way for easy access and communication, which abuses the privacy rights and increase cybercrimes to a peak.

The immense concern about the privacy and data protection has increased worldwide as a consequence of expansion in technology and online environment. So the surveillance potential of powerful computer systems prompt demands for specific rules governing the collection and handling of personal information. The protection of personal data is the key object of data protection which is the security of information and privacy in the computerized society.

So, the privacy is a right whilst data protection is the legislation which implements that right. Countries around the world have enacted different laws to protect the privacy of individuals. But in India, the right to privacy has been interpreted as an unarticulated fundamental right under the Constitution of India. The specific regulatory bodies seems to be lagging in aligning their policies to evolving security and privacy challenges. The Indian judiciary is in urgent need to take a pro-active role in protecting this right.

This paper proposed policy recommendations to the key entities that are in a position to make a difference in current state of the privacy and protection of data.

History

World's first computer specific statute was enacted in the form of a Data Protection Act, in the German state of Hesse, in 1970.

1) The misuse of records under the Nazi regime had raised concerns among the public about the use of computers to store and process large amounts of personal data.
2) The Data Protection Act sought to heal such memories of misuse of information. A different rationale for the introduction of data protection legislation can be seen in the case of Sweden which introduced the first national statute in 1973.
3) Here, data protection was seen as fitting naturally into a two hundred year old system of freedom of information with the concept of subject access (such a right allows an individual to find out what information is held about him) being identified as one of the most important aspects of the legislation.
4) In 1995, the European Union adopted its Directive (95/46/EC) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, the Directive), establishing a detailed privacy regulatory structure.
5) The Directive is specific on the requirements for the transfer of data. It sets down the principles regarding the transfer of data to third countries and states that personal data of EU nationals cannot be sent to countries that do not meet the EU "adequacy" standards with respect to privacy.
6) In order to meet the EU "adequacy" standards, US developed a 'Safe Harbour'.
7) Framework, according to which the US Department of Commerce would maintain a list of US companies that have self-certified to the safe harbor framework. An EU organization can ensure that it is sending information to a U.S. organization participating in the safe harbor by viewing the public list of safe harbor organizations posted on the official website.

Laws in India (Present Status)

Data Protection law in India is included in the Act [17] under specific provisions. Both civil and criminal liabilities are imposed for violation of data protection.

1) Section 43 deals with penalties for damage to computer, computer system etc.
2) Section 65 deals with tampering with computer source documents.

3) Section 66 deals with hacking with computer system.
4) Section 72 deals with penalty for breach of confidentiality and privacy. Call centers can be included in the definition of 'intermediary' and a 'network service provider' and can be penalized under this section.

These developments have put the Indian government under pressure to enact more stringent data protection laws in the country in order to protect the lucrative Indian outsourcing industry. In order to use IT as a tool for socio-economic development, employment generation and to consolidate India's position as a major player in the IT sector, amendments to the IT Act, 2000 have been approved by the cabinet and are due to be tabled in the winter session of the Parliament.

A landmark judgment with respect to this issue is **Kharak Singh v. State of U.P**. The Supreme Court held that the right of privacy falls within the scope of Article 21 of the Constitution and therefore concluded that an unauthorized intrusion in to a persons' home and disturbance caused to him is in violation of personal liberty of the individual.

However, in **Gobind v. State of Madhya Pradesh**, the Supreme Court qualified the right to privacy and held that a violation of privacy could be possible under the sanction of law.

The scope and ambit of the right of privacy or right to be left alone came up for consideration before the Supreme Court in **R. Rajagopal v. State of T.N.** during 1994. In this case the right of privacy of a condemned prisoner was in issue. By interpreting the Constitution in light of case law from the United Kingdom ("UK") and United States ("US"), Justice B.P. Jeevan Reddy held that though the right to privacy was not enumerated as a fundamental right, it could certainly be inferred from Article 21 of the Constitution.

Another significant case related to the right of privacy was the **People's Union of Civil Liberties v. the Union of India**. The case was primarily involved with the issue of 'telephone tapping' and held that tapping a person's telephone line violated his right to privacy, unless it was required in the gravest of grave circumstances such as public emergency.

While it may seem that the right to privacy is adequately protected as a fundamental right, it is essential to keep in mind that barring a few exceptions, fundamental fights secured to the individual are limitations only on State action. Thus, such an interpretation will not protect an individual against the actions of private parties.

The nine-judge bench of the Supreme Court has unanimously delivered its judgment in **Justice K.S. Puttaswamy (Retd.) v. Union of India**holding that privacy is a constitutionally protected right which not only emerges from the guarantee of life and personal liberty in Article 21 of the constitution, but also arises in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III of the Indian constitution.

The right to privacy judgment is one of the most landmark judgments of independent India. It not only learns from the past, but also sets the wheel of liberty and freedom for future. The Supreme Court of India has once again emerged as the sole guardian of the Indian constitution.

Issues Concerning Data Protection

1. Indian Economy Transforming to E-economy: While India is leading in providing IT services to businesses across the globe; the domestic sector has emerged as a key IT investor. Leading the pack, Government agencies are spending more than $ 10 billion in several of e-Governance. Internet penetration, although currently low at about 7.1 %, is rising exponentially.. According to the Celnet report, 'Payments in India is going e-way', E-transaction currently account for 30% of the total transactions, 75% of the total payment value is found in the electronic form. Indian IT and IT Services industry is growing multi-fold. According to Mckinsey-NASSCOM study, outsourcing industry currently at $60 billion, will reach to $225 billion by 2020. This transformation will increasingly bring Indian citizens under its fold, exposing them to the new age threats that not only have the potential to damage their financial interest, but also infringe their personal rights.

2. Privacy in New Age Transactions and Service Deliveries: Increasing commercialization in India that involves identifying potential customers, marketing products and services, promotional activities, and cross-selling is seen to be relying on the personal information. It has been observed that the data gathered while providing services and selling products is increasingly used for the purpose not intended. This has been more visibly observed in the telecom sector, which later resulted in the implementation of National Do Not Call Registry (NDNC). However, implementation of it on the ground remained abysmal, leading to irritation, frustration and worries of the end users. Privacy is slowly graduating into discussion landscape of India. However, in comparison to the advanced countries, the privacy initiatives both by individual companies and the respective regulatory bodies have remained at the surface

3. Cyber Crime and Warfare: Crime syndicates including terrorists are increasingly visible. New age cybercrimes increasingly attack the end users; increasing digitization of the end users' information aggravates this problem multifold. E-Governance applications are obvious targets of these attacks that come from cyber criminals or nation states, indulged into cyber warfare capabilities. Critical sectors like banking also offers lucrative target to them. This poses a great challenge to an individual, who is willingly or unwillingly, become a part of the cyber space. This lead to an unprecedented scene, where the significant section of population is exposed to grave threats that are international in nature.

4. National Security and Privacy: The proposed NATGRID -- a world-class integrated national security database -- will facilitate quick access to information on an individual -- like details of his/her banking, insurance, immigration, income tax, telephone and Internet usage. In the interest of sovereignty and integrity of India,

security of the State, the IT(Amendment) Act, 2008 authorized the designated agencies of Government to assume a power to issue directions for interception or monitoring or decryption of any information through any computer resource. This has a major bearing on privacy of an individual. Rising terrorism threats that India is witnessing in the recent years justifies a need for such monitoring of traffic, the implementation of ambitious projects such as NATGRID or Lawful Interceptions as allowed by amended IT Act may lead to infringement of the privacy of individuals.

5. Security and Privacy Challenges in a Centralized UID Database: Government of India has launched a massive project to issue unique identification numbers (UID Nos.) to all the residents of the country – close to 1.2 billion – by capturing their personal particulars along with biometrics such as fingerprints, iris scan and facial image. This has thrown up several privacy challenges. Data will be captured by thousands of registrars and sub-registrars throughout the country, sent over networks for storage centrally. Central data will be accessed for de-duplication whenever a new entry of UID is to be created. This poses privacy challenges at all stages of collection, processing and storage. These have been analyzed in detail in a paper prepared by Data Security Council of India (DSCI), 'Security and Privacy Challenges in the UID project'.

6. Outsourcing: Data Protection has emerged as a major challenge in cross-border data flows. Clients are demanding more security as their worries about the cybercrimes, privacy and identity theft grow. Regulatory and law-enforcement agencies of countries where clients are located require a proof of compliance by the IT/ITeS service providers (SPs) with their security and privacy regulations. Different countries have different laws to deal with data security and data privacy. While the European Union views privacy of personal information as a fundamental right, the United States has sector specific laws on privacy of the customer data. Processing of personal information of citizens of these countries by service providers (IT/BPO companies) in India and in other countries through outsourcing raises concerns about the regulatory compliance. In view of the multiplicity of privacy legislations worldwide, the service providers in India are faced with a major challenge of demonstrating compliance with the laws of countries where the data originate.

7. Arbitrary and unlawful interference: by the Government and private parties– The legislation must ensure that an individual's right to privacy is not interfered with in an arbitrary and unlawful fashion. Presently, judicial precedents prohibit violation of the right to privacy of an individual by Government agencies. A comprehensive law must provide for protection from intrusion by the Government as well as private parties.

It must also try and prohibit/curtail the use of cutting-edge technology to trespass upon privacy rights and personal data. Presently, the right to privacy on the Internet is being threatened due to several elements such as web cookies, unsafe electronic payment systems, Internet service forms, browsers and spam mail.

8. Medical records: Historically, medical records were used largely by physicians and medical insurers. However, with the creation of electronic records and large databases of medical information, the number of health care professionals and organizations with access to medical records has increased. It is essential that such data is not collected and sold to researchers in the field biomedical science, without the consent of the patients. With the advent of the internet, it has become increasingly difficult to track such data and not only does it amount to an invasion of privacy, but it also amounts to breach of the duty of confidentiality that medical professionals owe their patients.

9. Financial records: Financial records of individuals must also be protected from being distributed and circulated among banks and financial companies as it may also result in the misuse of such information.

International Standards

European Union (EU)

The European parliament and the Council of the EU passed the Data Protection

Distinct from all other major human rights, document protection of people's data has been included as one of the fundamental rights of the EU under Article 8 of the charter of the Fundamental Rights of the European Union. The EU directives are mainly aimed at facilitating the development of electronic commerce by fostering consumer confidence and minimizing differences between member state's data protection rules. The core data protection principle is the fair and lawful processing of personal information. The information must be obtained for one or more specified and lawful purposes and must be relevant to the purpose for which they are processed. The data should not be stored for longer than is necessary for the specified purpose. Further, both the controller and processor are under an obligation to enforce appropriate technical and organizational measures to protect against unlawful processing. The processor is subject to the same stringent conditions imposed on the controller, who remains under a further obligation to monitor the processor's compliance with the security measures for the durations of agency.

In order from the data controller the unclear impact of the "adequacy" standard on personal data transfers from the EU countries to other countries which do not have an act protecting privacy of all personal data transfers or an agency which monitored security of personal data, the other countries would be "inadequate" by European standards.

United States(US)

The United States has about 20 sector specific or medium-specific national privacy or data security laws and hundreds of such laws among its 50 states and its territories. California alone has more than 25 state privacy and data security laws.

In addition, the large range of companies regulated by the Federal Trade Commission(FTC) are subject to enforcement if they engage in materially unfair or deceptive trade practices. The FTC has used this authority to pursue companies that fail to implement reasonable minimal data security measures fail to live up to promises in privacy policies or frustrate

consumer choices about processing or disclosure of personal data. The FTC now considers information that can reasonably be used to contact or distinguish a person, including IP addresses and device identifiers, as personal data. The FTC has jurisdiction over most commercial entities and has authority to issue and enforce privacy regulations in specific areas (Ex. For telemarketing, commercial email and children's privacy).

Option rules apply in special cases involving information that is considered sensitive under US law, such as for health information, use of credit reports, student data, personal information collected online from children under 13, video viewing choices, precise geo location data, and telecommunication usage information.
The US also regulates marketing communications extensively, including telemarketing, text message marketing, fax marketing and email marketing. The first three types of marketing are frequent targets of class action lawsuits for significant statutory damages.

A few states have enacted laws imposing more specific security requirements for data elements that trigger security breach notice requirements. Both Nevada and Massachusetts laws impose encryption requirements on the transmission of sensitive personal information across wireless networks or beyond the logical or physical controls of an organization, as well as on sensitive personal data stored on laptops and portable storage devices.

HIPAA security regulations apply to so-called 'covered entities' such as doctors, hospitals, insurers, pharmacies and other health-careproviders, as well as their 'business associates' which include service providers who have access to, process, store or maintain any protected health information on behalf of a covered entity. 'Protected health information' under HIPAA generallyincludes any personally identifiable information collected by or on behalf of the covered entity during the course of providing its services to individuals. An important step taken in the US towards the protection of privacy on the Internet was the enactment of Children's Online Privacy Protection Act (COPPA). Under the rule, commercial websites and online services directed to children under 13 or that knowingly collect information from them must inform parents of their information practices and obtain verifiable parental consent29 before collecting, using, or disclosing personal information from children.

Japan

After European Union, Japan introduced a separate central legislation for protection of data as the Act on the Protection of Personal Information(APPI). The Act took partial effect in 2016 and has been enforceable from May 30, 2017. The law defines the scope of the legislation and states on whom the law is applicable under Article 2-4 of the APPI. As per the Act, it is applicable to four entities- state institutions, local public bodies, independent administrative agencies and an entity not having over 5,000 individuals' personal information for more than six months. Similar to the EU law, consent of a data subject forms the essence of the legislation and has been stated as

mandatory in case of transmitting data to a third party or for any use beyond communication purposes.

International Safe Harbour Principles

There was need to diminish the divide between the United States and the European Community who adopted different approaches to privacy protection to their citizens. Following extensive discussions, the EU Working Party and the US Department of commerce agreed that the department would compile a publicly accessible list of companies that provide adequate protection for personal data. Companies and individuals that subscribe to certain safe harbour principles will be able to secure protection against future data blockages.

The agreement between the European Union and the United States rests on seven safe harbour principles: notice, choice, onward transfer, security, data integrity, access and enforcement. India could incorporate these principles while formulating legislation in this behalf.

Notice - The data subject must be given notice in clear language, when first asked for personal data, of the purpose of data collection, the identity of the data controller, the kinds of third parties with whom the data will be shared, how to contact the organization collecting or processing the data, and the choices available for limiting use or disclosure of the information.

Choice - The data subject must be given clear, affordable mechanisms by which he or she can opt out of having personal information used in any way that is inconsistent with the stated purposes of collection.

Onward transfer - Where the data controller has adhered to the principles of notice and choice, it may transfer personal data if it ascertains that the receiving party also complies with the safe harbor principles, or if it enters into a contractual agreement that the receiving party will guarantee at least the same level of data protection as the transmitting party. When disclosure is made to a third party that will perform under instructions of the data controller, it is not necessary to again provide notice or choice, but the onward transfer principle continues to apply.

Security - The data controller must take reasonable precautions to protect data from loss or misuse, and from unauthorized access, disclosure, alteration or destruction.

Data integrity - The data controller must take reasonable steps to ensure that data are accurate, complete and current.

Access - Data subjects must have reasonable access to their personal data and an opportunity to correct inaccurate information.

Enforcement - At a minimum, enforcement mechanisms must include readily available and affordable recourse for the investigation of complaints and disputes, damages awarded where applicable, procedures for verifying the truthfulness of statements made by the data controller regarding its privacy practices, obligations of the data

controller to remedy problems arising out of noncompliance, and sanctions sufficiently rigorous to ensure compliance.

Recommendations

1) For the success of policy initiatives that can really create an impact, entities, including
2) Government and private, need to work in tandem. Each of these entities, in their respective
3) Capacity can bring the necessary change that promotes a culture of privacy.
4) Privacy by design is a trilogy model ewhuch could extend the encompassing application through
   i. IT systems;
   ii. Accountable business practices;
   iii. Physical design and infrastructure. It advocates a proactive approach, which relies on preventive measures of an organization to gain confidence to the end users. Data Security Council of India has come up with a privacy framework known as DSCI.
5) Privacy Framework which helps the organizations establish a privacy function that is based on visibility of information, intelligence over regulatory compliance, and privacy principles, policies and processes. Different frameworks, practices, technology measures and processes that embed into an organization's culture lead to a situation where privacy is treated as a hygiene factor in its operations.
6) End user education among the various measures that are advocated to build a privacy culture in India, education of end users is particularly important. Majority of them would be the first time users of the IT systems. With technology being seen as a means to achieve financial inclusion, there has been increased investment in the e-Governance projects. Simultaneously, growing private investment in the technology will bring the entire population of the country under the fold of cyber age. This is being done irrespective of how equipped the end users are to understand the dangers of the cyber space. End user's awareness of how his or her personal information is being collected, used, processed, shared and stored and how organizations and individuals can misuse this information will go a long way in creating a privacy culture. End user's awareness of the legal protection available to guard his or her personal rights , in case of any breach pertaining to the personal information, will definitely serve as an effective check on organizational practices in respect of processing the personal information. High level end user awareness will also help deploy trust mechanisms
7) The role of Self-regulation in data protection increasingly has been established as an effective step. Self-regulation reduces administrative bureaucracy and promises to bring efficiency in the data protection processes. A self-regulatory initiative has become now a useful instrument that not only supplements a legislative framework of an organization but also brings a required dynamism in the protection. United States has a long tradition of self-regulation. The best practices approach as a practical and realistic way to enhance global adherence to the data security standards.
8) Harmonize the legal framework which regulate communications surveillance in India to ensure that the law is accessible

and clear, and meets India's international human rights obligations;

9) Establish an independent and effective oversight mechanism with a mandate to monitor all stages of interceptions of communications to ensure they are compliant with India's domestic and international obligations to respect and protect the right to privacy and other human rights;
10) Establish independent accountability mechanisms and clear standards for India's security and intelligence agencies to ensure they are subject to independent oversight mechanisms and guarantee transparency of their mandate and operations in accordance with international human rights standards;
11) Review and reform the regulations regarding export and import of surveillance technologies to and from India and review all licensing agreements which impose obligations on the private sector to facilitate and/or conduct communication surveillance, and take the necessary measures to ensure that the private sector – in both policy and practice – comply with international human rights law and standards;
12) Review the proportionality of data retention requirements placed on telecommunications companies also adopt and enforce a comprehensive data protection legal framework that meets international standards, applies to both the private and public sector, and establish an independent data protection authority that is appropriately resourced and has the power to investigate data protection breaches and order redress.
13) Government of India, under the amended IT act, which is under progress, should set guiding principles for privacy in line with the globally recognized privacy principles. They can establish a national ecosystem that is continuously engaged for the data protection cause, issue guidelines and standards that provide practical guide government departments, e-Governance projects and private sectors and establish a mechanism for data breach notifications that mandates organizations to report the data breaches.
14) Attributes of humanity and democracy principles change with technology. Civil societies should proactively take data privacy in their agenda and vigilant review or monitoring of private organization's practices that processes personal information.
15) Augment skills to deal with technology matters that impact the end users under cyber security concepts and how cybercrimes are perpetrated, and develop investigative techniques for such crimes.
16) Issue specific and more granular set of guidelines and standards that control industry practices pertaining to processing of personal information.
17) Build a Risk and Compliance Intelligence mechanism that closely tracks global data protection regimes, and their impact on trans-border data flows.

Conclusion

The threat of privacy is also an obstacle towards facilitating a secure environment for communication over the Internet. Unless these issues are addressed India cannot take full advantage of the tremendous opportunities and benefits that e-commerce presents to developing nations such as ours.With the passage of time the 'global village' is being surrounded by and thickly

populated by these advancements and technology related developments where skies are the limit, therefore, every forthcoming minute is a challenge. Since it is always difficult to predict that what is going to happen in future but keeping in the view the desires of mankind and speed of technological innovation it can be said that the future is going to be more demanding and threats to our privacy and personal information are high which requires much effective data protection mechanism.

A legal framework needs to be established setting specific standards relating to the methods and purpose of assimilation of personal data offline and over the Internet. Consumers must be made aware of voluntarily sharing information and no data should be collected without express consent. India could also follow the regimes like those followed in other countries in order to overcome the data protection insecurities. The future of India's trade depends on striking an effective balance between personal liberties and secure means of commerce.

Reference

Data Protection Laws of the World- www.dlapiperdataprotection.com

The Right to Privacy in India: Stakeholder Report Universal Periodic Review 27th Session-India. By Centre for Internet and Society

India and Privacy International Act 2016

Marc Rotenberg, The Privacy Law Sourcebook, EPIC 1999: http://www.epic.org/bookstore/pls

Video Privacy Protection Act of 1988.

Guidelines on the Protection of Privacy and Trans Border Flows of Personal Data : http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM (As visited on April 18, 2002)

Kirby, Michael D "Privacy Protection – a New Beginning" 21st International Conference on Privacy and Personal Data Protection - Conference Proceedings 5.: www.pco.org.hk/conproceed.html (As visited in July 2001).

"US Report to Congressional Requesters on Medical Records Privacy" www.epic.org/privacy/medical/gao-medical-privacy399.pdf (As visited in July 2001).

Times of Indian http://timesofindia.indiatimes.com/india/CCS-seeks-tighter-privacysafeguards-in-NATGRID-proposal/articleshow/5557716.cms

*****